U.S. NAVAL ACADEMY
COMPUTER SCIENCE DEPARTMENT
TECHNICAL REPORT

IPv6 Testing

Landis, Christopher B

USNA-CS-TR-2006-02

May 8, 2006

Report Documentation Page

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **08 MAY 2006**	2. REPORT TYPE	3. DATES COVERED **00-05-2006 to 00-05-2006**

4. TITLE AND SUBTITLE **IPv6 Testing**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Naval Academy,Computer Science Department,572M Holloway Rd Stop 9F,Annapolis,MD,21403**	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES **10**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

IPv6 TESTING

Submitted by

Midshipman Christopher B. Landis, USN
073648

as independent research in conjunction with the
National Security Agency
and
Mr. Kevin Keeley
IA Solution Integration and Testing

_____

Midshipman Christopher B. Landis, USN

Faculty Advisor

_____

Professor Thomas R. Hendricks

Department Associate Chair

_____

Commander Thomas A. Logue, USN

1 May 2006

IPv6 TESTING

Midshipman 2/C Christopher Landis
United States Naval Academy

Appendix includes testing data.

1. <u>Abstract</u>. The DoD is committed to transitioning to Internet Protocol version 6 (IPv6) by 2008. Transitional working groups are under way to develop plans to implement IPv6 on Government networks. The DoD is also forming working relationships to conduct testing and share information.

2. <u>Background</u>. IPv6 was developed to resolve the issues of IPv4, mainly the limited amount of addresses and lack of security. The IPv6 address space has expanded from 32 bits (IPv4) to 128 bits (IPv6) creating 2^{128} unique addresses. It also provides end-to-end security using IPSec, adds mobility features and easier address management. The IPv6 testing team will have the opportunity to gain hands-on experience working with IPv6 heterogeneous networks and other teams enabling us to share resources and equipment. This IPv6 testing is necessary to evaluate interoperability and security issues that will arise in the transition, support and evaluations of IPv6 and dual-stack IPv6 and IPv4 networks.

3. <u>Goals</u>. The goal of this project will be to understand interoperability issues, security issues and configuration issues which will provide an understanding for system assessments and aid in the DoD transition. The use of IPv6 in commercial products and the features available will also be assessed. Results will be used to conduct evaluations. This testing will allow all involved to build expertise and understand the security issues in commercial as well as open source software. It will lead to the development of a best practices guide for transition and implementation as well as provide a direction for future research. At the end of the project, documentation will be provided on issues discovered and implementation guidance. Results will be presented in a final report at the end of testing activities.

4. <u>Methodology</u>.
   A. Testing will be conducted to analyze network activity through protocol analysis, stress testing, implementing diverse configurations and conducting vulnerability evaluations. By connecting to multiple internal and external labs through a virtual private network (VPN), a variety of configurations, equipment and network environments can be examined. These connections will extend the National Security Agency's capabilities by establishing partnerships with the military, DoD Agency's and the private sector. They will also allow for the sharing of IPv6 knowledge, leverage equipment and increase the type and amount of testing conducted in a shorter time period.
   B. The teams will analyze IPv4 to IPv6 transition methods, architecture security and configuration practices. Testing will identify issues surrounding IPv6 implementations, application implementation, and network tools and develop best practices for IPv6 configurations. Individuals on the teams will be able to apply a variety of tests against IPv6 using the multiple lab sites. Analysis will include both native IPv6 systems as well as mixed IPv6/IPv4 systems.

C. The test environments will include network routers and switches, operating system software and application software that can be used for testing in IPv6 only networks, tunneling IPv6 through IPv4 and in dual-stacked IPv4 and IPv6 networks. The team will investigate implementations of Microsoft Windows XP, Windows 2003, Windows Vista, Red Hat Linux Enterprise Edition, and Cisco IOS, each referred to as "XP," "2003," "Vista," "Red Hat," and "router," respectively.

D. Connections from remote sites will be made through VPNs to the IPv6 segment on the Agency network. The test segment will be a native IPv6 network. Remote connections will be made over the Internet and the segments at each site will also be native IPv6 networks. Participants will setup an IPv6 network with border routers running in a dual-stack mode to connect to the Internet.

5. <u>Conclusion</u>. IPv6 is not a new protocol. The main reason it has taken so long to be implemented is that its designers want IPv6 to fill its potential as the protocol to solve problems, not create problems. Over the past several years, multiple revisions of the protocol and RFC documents have theorized, written, and put in place to make IPv6 one of the most expansive protocols ever created. With each new feature, the opportunity for a security bug increases. It is crucial to national security that any areas in which security is lacking within IPv6 are found and fixes designed.

6. <u>Lessons Learned</u>. With the DoD committed to transitioning to IPv6 by 2008, it is crucial that the military be very aware of IPv6, its capabilities, and its security risks if implemented incorrectly. Through researching and testing IPv6, I now know a considerable bit about the protocol that most military members have not yet even imagined. The protocol must be tested and stretched to its limit with unique configurations and network topologies. In doing so, one can only learn more each day. As more and more learn about the inter-workings of IPv6, curriculum can be developed and knowledge can be propagated to those at the front lines so that they can take advantage of this versatile protocol.

Test 1: ICMP

Description: Monitor the traffic on the wire to identify the types of ICMPv6 packets that are required for Neighbor Discovery and Auto-Configuration to function.

Goal: Develop procedures for Neighbor Discovery and Auto-Configuration setup. Identify ICMPv6 messages required to still maintaining functionality.

Results: The only ICMPv6 type necessary for stateless AC is 134 (RA). Before assigning itself a global address, hosts will send out a router solicitation (ICMPv6 type 133) packet requesting a RA. Because of the access-list, the router solicitation packets are dropped at the router interface. It is not until the router sends an RA (in this case, every 20 seconds) does the host know which global prefix to use. ND does not require ICMPv6 type 135 or 136 (neighbor solicitation or neighbor advertisement, respectively), but neighbors can be discovered through types 128 and 129, echo request and echo reply. The Cisco 3640 Router can be setup to accomplish this with the following configuration:

```
interface FastEthernet3/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:1918:201:10::1111/64
 ipv6 enable
 ipv6 traffic-filter test1-4 in
 ipv6 traffic-filter test1-4 out
 ipv6 nd ra-interval 20
 ipv6 nd prefix 2001:1918:201:10::/64 86400 86400
ipv6 access-list test1-4
 remark RAs
 permit icmp any any router-advertisement
 remark ping test
 permit icmp any any echo-reply
 permit icmp any any echo-request
```

Security Issues:
      XP will gain several IPv6 global addresses simultaneously during its time on the network. Using up available addresses is not a valid concern in IPv6, however, one must consider the reasoning for host renumbering (HR). HR makes it more difficult to track PCs and their actions on the network, thus increasing stealth. In this test, the expiration was 24 hours and some global addresses would be a week old. There are two ways to think about this situation: 1. An address can be tracked for seven times the duration of the set expiration. 2. Having seven different addresses, if each used randomly, can be most difficult to track.
      Of the four operating systems, Vista best follows RFC 2426 (on IPv6 Stateless Address AC).
      2003 and Red Hat do not work well with stateless AC. Globally, each assigns only one address with embedded MAC. Therefore, the address never changes or expires. Tracking these systems' network activity is relatively easy.

Test 1.1

Test Setup: All PCs (XP, 2003, Red Hat) are running dual-stack. XP has no IPv6 manually assigned addresses. 2003 and Red Hat have manually assigned IPv6 addresses. Ethereal server has no IPv6 installed.

Procedure: Boot one PC on at a time while monitoring traffic on Ethereal.

Results: Test is considered failure because RAs were not configured properly. Global IPv6 addresses were not being generated on the PCs.

Test 1.2

Test Setup: All PCs are running dual-stack. The router is the only manually assigned IPv6 address on the LAN. Configured with the following four commands on a fast Ethernet interface:
- `ipv6 address 2001:1918:201:10::1111/64`
- `ipv6 enable`
- `ipv6 nd ra-interval 20`
- `ipv6 nd prefix 2001:1918:201:10::/64 86400 86400`

Ethereal server has no IPv6 installed.

Procedure: Boot one PC on at a time while monitoring traffic on Ethereal.

Results: Auto-configuration was successful. XP gained an additional address every 24 hours (expiration time on AC). The other addresses remained and were able to be pinged because each address is attached to the link-local address of the interface. Is this not a security problem for XP users?

Test 1.3

Test Setup: All PCs (Vista added bringing the count to 4 clients) are running dual-stack. The router is the only manually assigned IPv6 address on the LAN. Ethereal server has no IPv6 installed.

Procedure: Boot one PC on at a time while monitoring traffic on Ethereal.

Results: Auto-configuration was successful. The assigned gateway for all PCs was the router's link-local address.

XP gained an additional address every 24 hours (expiration time on AC) with a maximum of 9 IPv6 addresses (1 link-local, 1 global with MAC embedded, and up to 7 global). All 9 are able to be pinged by other hosts on the LAN. As the most recent of the 7 rotating global address addresses expired, a new IPv6 address would be assigned and the oldest of the 7 would no longer be accessible on the LAN; it is a FIFO queue. All addresses that were ever assigned to XP are viewable in the "netsh interface ipv6>show neighbors" command. The 9 current addresses are all marked as "Permanent" and all other addresses that were once assigned but are no longer available, are marked as "Incomplete" and have no physical address assigned. Also listed in the IPv6 neighbors table are the router's link-local and manually assigned global address, marked as

"Stale." The link-local and an old global with MAC addresses are also shown in XP's neighbors table. This is likely here because of a ping that occurred more than 24 hours previous. XP needs to empty its cache more often.

Vista has a total of 3 IPv6 addresses: 1 link-local, 1 temporary global, and 1 permanent global (with embedded MAC address). The 1 temporary global address does not change or regenerate after the 24-hour expiration period set in the RAs. Instead, it assigned itself a new IPv6 temporary global address after a longer, undetermined period of time. The "netsh interface ipv6>show neighbors" command displays link-local and global addresses for all neighbors and itself. Vista does not seem to clear its cache of old or unreachable IPv6 addresses. Any addresses of other PCs only appear because of earlier pings.

2003 has two IPv6 addresses: 1 link-local and 1 global with embedded MAC. There is no IPv6 address that changes every 24 hours. The IPv6 neighbors consist only of itself and the router with both link-local and global addresses. 2003 did not send or receive any pings so there are no other hosts listed in the neighbors.

Red Hat has two IPv6 addresses: 1 link-local and 1 global with embedded MAC. There is no IPv6 address that changes every 24 hours. The IPv6 neighbors consist only of the router's link-local address.

Test 1.4

Test Setup: All PCs are running dual-stack. The router is the only manually assigned IPv6 address on the LAN. Configured with an ACL permitting ICMPv6 types 128 (echo request), 129 (echo reply), and 134 (RA) and the additional two commands on a fast Ethernet interface:

- ```
  ipv6 access-list test1-4
  remark RAs
  permit icmp any any router-advertisement
  remark ping test
  permit icmp any any echo-reply
  permit icmp any any echo-request
  ```
- ```
  ipv6 traffic-filter test1-4 in
  ```
- ```
  ipv6 traffic-filter test1-4 out
  ```

Ethereal server has no IPv6 installed.

Procedure: Boot one PC on at a time while monitoring traffic on Ethereal.

Results: Auto-configuration was successful. All four PCs reacted exactly the same as in Test 1.3.

Test 1.5

Test Setup: All PCs are running dual-stack. All test equipment (PCs and router) is off. Ethereal server has no IPv6 installed.

Procedure: Boot only one PC at a time while monitoring traffic on Ethereal. Check ipconfig and IPv6 neighbors to ensure no global addresses were cached. Shutdown each PC before starting the next.

Results: Test was successful. All four PCs were only configured with link-local addresses.

Test 2: AC

Description: Stateless Auto-Configuration can query for Stateful Auto-Configuration services on the local network to allow it to determine its own global IPv6 address, net prefix, and default routers. Enable Stateful Auto-Configuration then enable Stateless Auto-Configuration. Identify the security issues that are present, which would allow users to gain an address on the network. What countermeasures will prevent this? What information is passes on the wire? Will Duplicate Address Detection detect the spoofed address? Can the client self configure a link local address then pull subnet and gateway information from the router with limited ICMP traffic?

Goal: Determine whether Duplicate Address Detection detects the spoofed address, if any user can connect to the network, and which traffic is required on the network. Develop successful countermeasures.

Results: Stateful AC (DHCPv6) has yet to be successful. As an IPv6 potential client connects to the network, one of the first packets it sends is an RS. If there is no reply or the reply RA is not set for auto configure, the client is satisfied with only having a link-local address. If a RA is configured for managed configuration, the host is supposed to get its address from a DHCPv6 server (the router) in a Stateful manner. If a RA flag is configured for additional information, the host is supposed to get other network settings like DNS from the DHCPv6 server.

Security Issues: Not much can be seen here until the Stateful AC is working properly.

Test 2.1

Test Setup: All PCs are running dual-stack. Router is configured to hand out address through Stateful AC and not Stateless AC. Ethereal server has no IPv6 installed.

Procedure: Boot only one PC at a time while monitoring traffic on Ethereal.

Results: Test considered failure. PCs are configured via stateless AC.

Test 2.2

Test Setup: All PCs are running dual-stack. Router is configured to hand out address through Stateful AC and not Stateless AC. ACL implemented to deny RAs. Ethereal server has no IPv6 installed.

Procedure: Boot only one PC at a time while monitoring traffic on Ethereal.

Results: Test considered failure. PCs are configured via stateless AC. ACL has no effect on RAs.

Test 2.3

Test Setup: All PCs are running dual-stack. Router is configured to hand out address through Stateful AC and not Stateless AC. ACL implemented to deny RS and RA packets. Ethereal server has no IPv6 installed.

Procedure: Boot only one PC at a time while monitoring traffic on Ethereal.

Results: Test considered failure. PCs are configured via stateless AC after a few-minute delay due to lack of RAs (default RA broadcast is 200 seconds). Since RS packets are getting denied, the router does not have RS packets to reply to RAs. ACL has no effect on RAs.

Test 2.4

Test Setup: All PCs are running dual-stack. Router is configured to hand out address through Stateful AC and not Stateless AC. ACL implemented to deny RS and RA packets. Manage-config-flag and RA suppression are set. Ethereal server has no IPv6 installed.

Procedure: Boot only one PC at a time while monitoring traffic on Ethereal. After no PCs are configured with global IPv6 addresses, RA suppression and ACL are removed.

Results: Test considered failure. PCs are configured via stateless AC.

Test 2.5

Test Setup: All PCs are running dual-stack. Router is configured to hand out address through Stateful AC and not Stateless AC. Manage-config-flag is set. Ethereal server has no IPv6 installed.

Procedure: Monitor traffic on Ethereal while changing router configurations for packet manipulation. Boot PCs as needed to test DHCPv6 capability.
Real-time procedure:
1. RA interval set to 10 seconds.
2. Power up Red Hat to generate RS traffic, in hopes of router replying with RAs.
3. Set router prefix to 300 seconds preferred and valid lifetime and set no-auto-config flag.
4. Enable unicast-routing on router.
5. Enable multicast-routing on router.
6. Set other-config-flag.
7. Set NS-interval to 20000 milliseconds.
8. Set RA-lifetime to 30 seconds.
9. Power up Vista to generate RS traffic and to test current configuration.
10. Set no-rtr-address flag (no router address).
11. Set off-link tag in prefix command.
12. Remove other-config-flag.
13. Remove off-link flag.
14. Set other-config-flag.

15. Remove managed-config-flag.
16. Set managed-config-flag.
17. Power up 2003.
18. Restart Vista.

Results: Test considered failure. PCs are configured via stateless AC. No IPv6 traffic initially on network. Stateful AC does not seem to work yet. The off-link flag determines whether a host only needs an RA to consider the router a neighbor or if a NA is needed from the router. If the no-auto-config flag is set, then there will be no AC, stateful or stateless.

Results after same procedure step:
1. Still no IPv6 traffic.
2. No reply traffic from router.
3. No change.
4. RAs broadcasts start.
5. PIMv2 "Hello" broadcasts start.
6. No change.
7. No change.
8. No change.
9. Neither Vista nor Red Hat are configured with global IPv6 addresses.
10. No change.
11. Router's global address is not in any PC's neighbors list; only the router's link-local is in the PC's neighbors list.
12. No change.
13. No change.
14. No change.
15. Almost instantly, the router sends an NS packet to Vista and the router's global address is now in the Vista neighbors. Vista replies with NA packet and also sends NS packet to router. Router replies with NA packet.
16. No change.
17. 2003 configured via stateless AC.
18. Vista configured via stateless AC.